

①

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-187306

(43)Date of publication of application : 02.07.2004

(51)Int.Cl.

H04L 9/16  
H04L 12/56  
H04N 7/08  
H04N 7/081  
H04N 7/16

(21)Application number : 2003-406448

(71)Applicant : IRDETO ACCESS BV

(22)Date of filing : 04.12.2003

(72)Inventor : RANJAN KARTHIK

(30)Priority

Priority number : 2002 02080137

Priority date : 04.12.2002

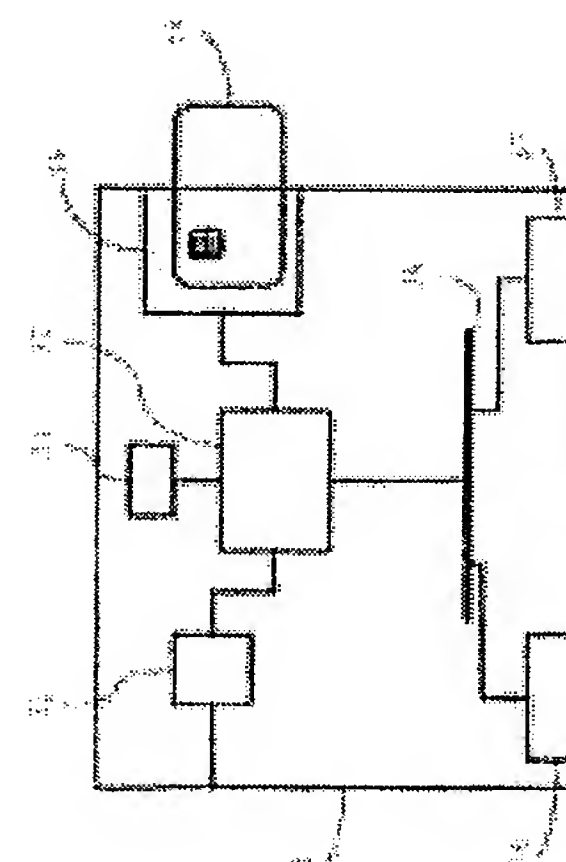
Priority country : EP

(54) TERMINAL FOR RETRANSMITTING DIGITAL DATA, TERMINAL WITH METHOD THEREOF, AND DATA DISTRIBUTION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a terminal for receiving and retransmitting information.

SOLUTION: The present invention provides a first network adapter (31, 36) for encoding information to receive a first data stream encrypted by a key scheme from a first transmitter (25, 26, 27) via a first network within a first format, a device for receiving an entitlement message to enable an authorized receiver to decrypt the encrypted data stream, and at least another network adapter (37) for connection to a second network (2).



(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号  
特開2004-187306  
(P2004-187306A)

(43) 公開日 平成16年7月2日(2004.7.2)

(51) Int. Cl. <sup>7</sup>	F I	テーマコード (参考)
HO4L 9/16	HO4L 9/00 643	5C063
HO4L 12/56	HO4L 12/56 Z	5C064
HO4N 7/08	HO4N 7/16 Z	5J104
HO4N 7/081	HO4N 7/08 Z	5K030
HO4N 7/16		

審査請求 未請求 請求項の数 15 O L (全 15 頁)

(21) 出願番号	特願2003-406448 (P2003-406448)	(71) 出願人	500232617 イルデト・アクセス・ベー・フェー オランダ・NL-2132・HD・フーフ ドドープ・ジュピターストラート・42
(22) 出願日	平成15年12月4日 (2003.12.4)	(74) 代理人	100064908 弁理士 志賀 正武
(31) 優先権主張番号	02080137.9	(74) 代理人	100108578 弁理士 高橋 昭男
(32) 優先日	平成14年12月4日 (2002.12.4)	(74) 代理人	100089037 弁理士 渡邊 隆
(33) 優先権主張国	欧州特許庁 (EP)	(74) 代理人	100101465 弁理士 青山 正和
		(74) 代理人	100094400 弁理士 鈴木 三義

最終頁に続く

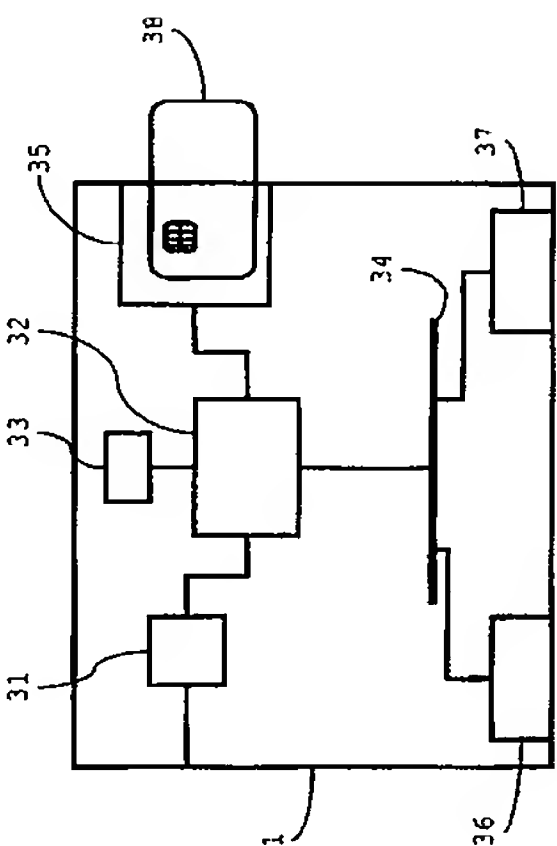
(54) 【発明の名称】 デジタルデータを再送信する端末及び方法を具備する端末及びデータ配信システム

(57) 【要約】

【課題】 情報を受信及び再送信するための端末を提供する。

【解決手段】 情報が符号化され、第1フォーマット内の第1ネットワークを介して第1送信器(25, 26, 27)からのキースキームによって暗号化された第1データストリームを受信するための第1ネットワークアダプタ(31, 36)と、認可された受信器が前記暗号化データストリームを解読できるようにするエンタイトルメントメッセージを受信するための装置と、第2ネットワーク(2)へ接続するための少なくとも1つの別のネットワークアダプタ(37)とを備える。

【選択図】 図3



## 【請求項 9】

前記端末は、第 1 フォーマット内の符号化された情報を具備する第 1 データストリームを受信し、第 2 フォーマット内に前記情報を符号化し、少なくとも 1 つの前記第 2 データストリーム内に再符号化された前記情報を具備するデータを含むように構成されることを特徴とする請求項 1 ないし請求項 8 のうちいずれか 1 に記載の端末。

## 【請求項 10】

前記端末は、第 1 スキームに基づいて圧縮されたデータを具備する第 1 データストリームを受信し、前記データを逆圧縮し、第 2 スキームに基づいて前記データを再圧縮し、少なくとも 1 つの前記第 2 データストリーム内の再圧縮された前記データを含むために実施されることを特徴とする請求項 9 に記載の端末。

10

## 【請求項 11】

前記端末は、少なくとも 1 つの前記第 2 端末(3, 5, 6)に少なくとも 1 つの前記第 2 データストリームの送信を認可するメッセージを受信し、権限が受信されるそれらの第 2 端末(3, 5, 6)にそれら第 2 データストリームのみを送信するように構成されることを特徴とする請求項 1 ないし請求項 10 のうちいずれか 1 に記載の端末。

## 【請求項 12】

認可された受信器が前記キースキームによって暗号化された暗号化データストリームを解読することができる複数の異なるエンタイトルメントメッセージを受信するための装置を備え、前記エンタイトルメントメッセージそれぞれは、少なくとも 1 つの端末の規格を備え、

20

前記端末は、前記第 2 端末(3, 5, 6)が一致する規格を具備するそれらのエンタイトルメントメッセージのみ、前記第 2 端末(3, 5, 6)に転送するように構成されることを特徴とする請求項 1 ないし請求項 11 のうちいずれか 1 に記載の端末。

## 【請求項 13】

第 1 ネットワークと、

前記第 1 ネットワークに接続されるとともに、第 1 フォーマット内の前記第 1 ネットワークを介したキースキームによって暗号化された暗号化第 1 データストリーム内で符号化された情報を送信するように構成される第 1 データ送信器(25, 26, 27)と、

認可された受信器が前記暗号化データストリームを復号化できるようなエンタイトルメントメッセージを送信するように構成されるエンタイトルメントメッセージ送信器(25, 26, 27)と、

30

第 2 ネットワーク(2)と、

前記第 2 ネットワーク(2)に接続された 1 つまたはそれ以上の第 2 端末(3, 5, 6)と、

前記第 1 ネットワークおよび前記第 2 ネットワーク(2)に接続され、前記第 1 ネットワークを介して前記第 1 データ送信器(25, 26, 27)から前記暗号化データストリームを受信するとともに、前記第 1 フォーマットと異なる第 2 フォーマット内の少なくとも 1 つの第 2 データストリーム内で符号化された前記情報の少なくとも一部を、前記第 2 ネットワーク(2)に接続された 1 つまたはそれ以上の第 2 端末(3, 5, 6)に再送信するように構成される第 1 端末(1)とを備え、

前記第 1 端末(1)は、同じキースキームによって暗号化された前記第 2 データストリームを送信するとともに、認可された受信器が前記第 2 端末(3, 5, 6)への前記第 2 データストリームを解読できる受信エンタイトルメントメッセージを転送するように構成されることを特徴とするデジタルデータ配信システム。

40

## 【請求項 14】

第 1 フォーマット内の第 1 ネットワークを介した第 1 送信器(25, 26, 27)からのキースキームによって暗号化された暗号化第 1 データストリーム内で符号化された情報を受信する段階と、

認可された受信器が前記暗号化データストリームを解読できるエンタイトルメントメッセージを受信する段階と、

前記第 1 フォーマットと異なる第 2 フォーマット内の少なくとも 1 つの第 2 データスト

50

具備する。

【0004】

また、本発明は、デジタルデータを受信及び再送信する方法に関し、前記方法は、第1フォーマット内の第1ネットワークを介した第1送信器からのキースキームによって暗号化された暗号化第1データストリームで符号化された情報を受信する段階と、認可された受信器が前記暗号化データストリームを解読できるようなエンタイトルメントメッセージを受信する段階と、前記第1フォーマットと異なる第2フォーマット内で少なくとも1つの第2データストリーム内に符号化された前記情報の少なくとも一部を、第2ネットワークを介して少なくとも1つの第2端末に再送信する段階とを備える。

【0005】

さらに、本発明は、デジタルデータを受信及び再送信するための端末にローディングするのに適したコンピュータプログラムに関し、前記端末は、プロセッサと、メモリと、第1フォーマット内の第1ネットワークを介して第1送信器からデータストリームを受信するための第1ネットワークアダプタと、認可された受信器が暗号化データストリームを解読できるようなエンタイトルメントメッセージを受信するための装置と、第2ネットワークに接続するための少なくとも1つの別のネットワークアダプタとを備える。

【背景技術】

【0006】

そのような端末、システム及び方法の例は、例えば、特許文献1によって公知である。この公報には、ビデオケーブル及びIEEE 1394ケーブルを介してテレビジョン受信器に接続されるセットトップボックスが開示されている。フロントエンド回路(front end circuit)は、ユーザの局選択に対応する放送信号を、アンテナからのDSS(ダイレクト衛星システム(Direct Satellite System))入力から抽出するとともに、デスクランブル回路(descramble circuit)にそれを出力する。充電回路は、スクランブル解除のための復号化キーを前記デスクランブル回路に供給する。マルチプレクスエディティング回路(多重化編集回路(multiplex editing circuit))は、タイムスタンプ及び(MPEG符号化された)HD放送信号のパケット長さを、前記デスクランブル回路からIEEE 1394で定義されたトランスポートストリームに再配置(rearranges)するとともに、次いで、暗号化回路にそれを出力する。関係している(concerned)前記放送信号がペイパービュー(pay per view)である場合、前記暗号化回路は、前記マルチプレクスエディティング回路からの前記トランスポートストリームを暗号化する。コントローラは、磁気ディスク、光ディスク、光磁気ディスクまたは半導体メモリに記憶された制御プログラムを読み出すためにドライブを制御するとともに、読み出された前記制御プログラム及びユーザからのコマンド入力などに基づいて、前記セットトップボックスの各回路を制御する。前記充電回路は、前記暗号化回路に接続されていない。

【0007】

前記公知端末が用いられるとき、前記第1送信器からのエンティティ(entity)送信データは、前記データが前記第1端末で解読されるとすぐに制御を解除する。次に、前記復号化データが再暗号化されたとしても、このエンティティは、もはや前記データへのアクセスを制御しない。前記第2ネットワークを介した前記データの受信及び再送信のために用いられる前記第1端末のオペレータは、前記データストリームを再暗号化するために用いられたキーをそれらに送信することによって、前記再暗号化データストリームの解読が可能な第2受信器を決定できる。

【0008】

【特許文献1】ヨーロッパ特許公開公報1089470

【発明の開示】

【発明が解決しようとする課題】

【0009】

本発明は、デジタルデータの第1提供者が第2ネットワークを介して前記データの別の配信の制御を実行し続けることができるような、上述のタイプの端末、システム及び方法

10

20

30

40

50

本発明の別の形態によると、デジタルデータを受信及び再転送する方法が提供される。デジタルデータを受信及び再転送する方法は、第1フォーマット内の第1ネットワークを介した第1送信器からのキースキームによって暗号化された暗号化第1データストリーム内で符号化された情報を受信する段階と、認可された受信器が前記暗号化データストリームを解読できるようなエンタイトルメントメッセージを受信する段階と、前記第1フォーマットと異なる第2フォーマット内の少なくとも1つの第2データストリーム内で符号化された前記情報の少なくとも一部を、第2ネットワークを介して少なくとも1つの第2端末に再送信する段階とを備え、前記第2データストリームは、前記同じキースキームによって送信され、暗号化され、そして、認可された受信器が前記第2データストリームを解読できるような受信されたエンタイトルメントメッセージが前記第2端末に転送される。

10

【0017】

これは、本発明による前記端末によって実行される方法である。

【0018】

本発明の最後の形態によると、デジタルデータを受信及び再送信するための端末にローディングするのに適したコンピュータプログラムが提供され、前記端末は、プロセッサと、メモリと、第1フォーマット内の第1ネットワークを介して第1送信器からデータストリームを受信するための第1ネットワークアダプタと、認可された受信器が暗号化データストリームを復号化できるようなエンタイトルメントメッセージを受信するための装置と、第2ネットワークに接続するための少なくとも1つの別のネットワークアダプタとを備える。故に、この方法でプログラムされた端末は、本発明による端末の前記機能が提供される。

20

【0019】

従って、前記正当なハードウェアを伴う端末は、エンドユーザに至るまで前記コンテンツの配信を制御するさらなる確実性を、コンテンツ提供者に提供する本発明による端末としての機能に容易に適合される。

【発明を実施するための最良の形態】

【0020】

ここで、本発明は、添付の図面を参照してさらに詳細に説明される。

【0021】

図1を参照すると、本発明は、2つのネットワーク、すなわち、この例では、配信ネットワークとホームネットワーク2との間のゲートウェイとして用いられる第1受信器1を提供する。前記第1受信器1は、第1フォーマットでデータを受信するとともに、第2フォーマットでそれを再送信する。本発明は、シングルタイプのデータに限られるものではないが、この説明においては、MPEG-2トランスポートストリームパッケージが、前記ホームネットワーク2を介して複数の第2受信器にそれら（データ）を再送信する前記第1受信器1に配信される例に焦点をあてる。図1に示されるように、第2受信器の例は、アナログテレビジョンセット4に接続されるセットトップボックス3と、デジタルテレビジョンセット5と、パーソナルコンピュータ6とである。パーソナルコンピュータ6は、ネットワークカードと、メディアプレイヤーと、スマートカードリーダー7とを備える。また、本発明は、放送環境に用いられるとは限られない。すなわち、前記第1受信器1は、また、ポイントツ

30

40

【0022】

前記MPEG-2スタンダードISO/IEC 13818はある程度詳しく、データ符号化方法及び転送方法について記載している。この記載は、本発明に関する他の形態を本質的に詳述する。標準についてさらに詳細に知るためには、参照する必要があるかも知れない。

【0023】

図1において、放送ソース8は、基本ストリーム9をシングルプログラムMPEG-2トランスポートストリーム10に符号化する。基本ストリームは、例えば、ビデオまたはオーディオのようなプログラムの、単にデジタルコード化されるとともに、MPEG-圧縮されたコンポーネントである。プログラムに属するいくつかの基本ストリームからのデータは、プログ

50

ストリームレベルで実行されるものと仮定する。好適には、DESのような対称暗号化アルゴリズムが前記TSパケットペイロード17をスクランブルするために用いられる。

#### 【0029】

PID値に関係なく、同一のキー及び/またはアルゴリズムを使って前記TSパケットペイロード17全てをスクランブルすること、または、各基本ストリームまたは1つのプログラムに属する基本ストリームの各セットに対して、異なるキー及び/またはアルゴリズムを用いることが可能であることが知られている。前記総括局22がCAシステムマネージャであると仮定すると、それは、エンタイトルメント制御メッセージを含む1つまたはそれ以上のトランスポートストリームをサプライスする。さらに、CAシステムで用いられるタイプ及び前記エンタイトルメントメッセージの前記PIDを詳細したCA記述子をそれに追加することによって、スクランブルされた前記プログラムに対する前記PMTを修正する。前記エンタイトルメント制御メッセージは、制御語、スクランブリング及びデスクランブリングのために用いられるキーを具備している。エンタイトルメント制御メッセージ(ECMs)は、異なったキーによってそれら自身を暗号化する。別のデータストリームは、認可された加入者または加入者のグループが、前記制御語を取り出せる前記ECMsを解読できるようなエンタイトルメントマネージメントメッセージ(entitlement management messages)を具備する。

10

#### 【0030】

図1に戻ると、第1受信器1は、それ(第1受信器)が接続される衛星放送受信アンテナ30によって前記MPEG-2トランスポートストリームを受信する。前記トランスポートストリームは、衛星配信ネットワークを介した送信に適したフォーマット、例えば、DVB-S(Digital Video Broadcasting-Satellite)に対するコンフォーマント(conformant)である。前記第1受信器1は、異なるフォーマットでデータが送信されるが、前記ホームネットワーク2を介して、前記データの一部または全部を端末装置で使えるようにする。従って、前記第1受信器1は、配信ネットワークゲートウェイ、すなわち1つまたはそれ以上の配信ネットワークと、1つまたはそれ以上のホームネットワークセグメントに接続される装置である。前記配信ネットワーク(すなわち、前記衛星ネットワーク)がOSI層のいずれかにおいて前記ホームネットワークセグメントに相互接続されるように、それは、1つまたはそれ以上の接続コンポーネントを含んでいる。それは、異なるリンク層技術を相互接続するブリッジまたはルータとして機能できる。すなわち、前記OSI4層以上における機能性も提供するゲートウェイとしての役割を果たせる。結果として、フォーマットという用語は、ネットワークのあるタイプのプロトコルスタックに前記データが一致するよう適合させる方法を意味している。第1ネットワーク(前記衛星ネットワーク)は、前記リンク層レベル、前記ネットワーク層レベルまたは前記トランスポート層レベルのうちの1つまたはそれ以上で異なっていることを意味している前記ホームネットワーク2と異なるプロトコルスタックを有している。ここで留意すべきことは、データがフレーム及び/またはパケットで送信される前記第1受信器1は、前記ホームネットワーク2の前記プロトコルスタックと一致するために、パケットヘッダ及び/またはリセグメント(re-segment)パケットペイロードを追加、除去または変更しなければならない。前記パケットという用語は、通信ネットワーク内のユニットとして送信されるデータの小区間である(refer to)。それは、セルとして知られるパケットのタイプだけでなく、フレームとして一般的に知られる前記ネットワーク層より下のレベルでのパケットを含んでいる。パケットは、ヘッダまたはトレーラ(trailer)と、ペイロードとを具備する。パケットフォーマットは、前記ペイロードの大きさに関するとともに前記ヘッダ/トレーラに含まれる種々のフィールドに関する前記パケットの構成である。

20

30

40

#### 【0031】

図3は、前記第1受信器1のコンポーネントを概略的に示している。それ(第1受信器1)は、前記MPEGトランスポートストリームを具備するベースバンド信号を取り出すために、搬送波を除去するチューナー/復調器31を備える。前記第1受信器1は、前記パケットを処理するためにプロセッサ32及びメモリ33を用いる。前記プロセッサ32は、システムバス

50

IPヘッダ41)は、マルチキャストアドレスを備えてもよい。前記IPパケット39は、プリアンブル43、宛先アドレス44、ソースアドレス45、タイプ46及びCRCチェックサム(checksum)47を備えるイーサネット(登録商標)フレーム42の前記ペイロードを形成する。前記宛先アドレス44は、それらを目的とする前記イーサネット(登録商標)フレームを取り出すために、前記第2受信器によって用いられるブロードキャストアドレス、マルチキャストアドレスまたはユニキャストアドレスである。IP及びUDPヘッダ41,40を付加せずに、前記イーサネット(登録商標)フレーム42内の前記TSパケット14を直ちにカプセル化することも可能であることが知られている。しかしながら、イーサネット(登録商標)を介してIPを用いることは、広範囲に渡って前記データを送信することを可能にする。

【0036】

好適には、出願人の同時係属国際出願W0 02/07378に全面的にさらに記載されているように、前記第1受信器1は、前記スタックのもとで暗号化の一形態を用いる。

【0037】

本発明の好適な実施形態では、前記第2受信器は、前記ホームネットワーク2を介して前記第1受信器1に選択コマンドを送信することができる。これらの選択コマンドへの応答において、前記第1受信器1は、いかなる前記第2受信器によっても要求されない前記マルチプログラムトランスポートストリーム内のそれらの基本ストリームを、フィルタをかけて除去する。従って、それ(前記第1受信器)は、各第2受信器に基本データストリームのサブセットのみ送信することができる。

【0038】

また、前記第2受信器のそれぞれは、スマートカードリーダを備える。挿入されたスマートカードは、それら(前記第2受信器のそれぞれ)が前記第1受信器1から受信されたデータのストリームから複数の前記ECMを取り出すとともに、ある基本ストリームをデスクランブルすることができるようにする。

【0039】

また、前記第1受信器1は、前記モデム36を用いて前記TSパケットを受信できる。この場合、前記TSパケットは、IPパケット内ですでにカプセル化されていてもよい。しかしながら、複数のイーサネット(登録商標)パケット内でカプセル化される代わりに、前記受信されたIPパケットは一般的に、前記リンク層レベルでPPPパケットまたはATMセルに運び込まれる。それ故に、前記第1受信器1は、イーサネット(登録商標)フレームフォーマット内の受信されたデータを再送信するために、本発明による方法を実行しなければならない。

【0040】

上記のように、前記第1受信器1は、解読されたデータストリームを再パケット化する。本発明の範囲内で、前記第1受信器1の別の変形が可能である。この変形例では、前記第1受信器1は、第1フォーマット内の符号化された情報を備える第1データストリームを受信し、第2フォーマット内の前記情報を再符号化し、前記第2データストリームの少なくとも1つで前記再符号化された情報を備えるデータを含むように構成される。このいわゆるトランスコーディング(transcoding)は、前記受信されたデータの非圧縮(伸長)及び再圧縮を必要とする可能性がある。一例として、前記第1受信器1は、前記MPEG-4標準により符号化及び圧縮されたプログラム基本ストリームを取り出すためにトランスポートストリームを逆多重化してもよいし、前記符号化されたビデオデータを逆圧縮してもよいし、前記MPEG-2標準によって前記ビデオデータを再圧縮及び符号化してもよい。次いで、トランスコードされた(transcoded)ビデオデータは、パケット化されるとともに前記1つまたはそれ以上の第2受信器に送信されるトランスポートストリーム内にオーディオ及びデータを含んでいる他の関連プログラム基本ストリームによって、多重化される。当然ながら、MPEG-4からMPEG-2へのトランスコーディングは、まさに好都合な例である。データが再送信される場合、前記第1受信器1は、静止画像を、例えば、JPEGからGIFにトランスコードするように構成される。これらの実施形態は、前記第2受信器によってサポートされない異なったフォーマットに放送局が切り換られた場合、第2受信器としてレガシー

10

20

30

40

50

1 3	PESパケットペイロード	
1 4	MPEG-2 TSパケット	
1 5	MPEG-マルチプレクサ	
1 6	TSパケットヘッダ	
1 7	TSパケットペイロード	
1 8	適応フィールド	
1 9	パケット識別子	
2 0、2 3、2 8、2 9	ネットワークアダプタ	
2 1	第1ネットワーク	
2 2	総括局	10
2 4	ビットストリーム/マルチプレクサ	
2 5	衛星送信器	
2 6	地上送信器	
2 7	ケーブル送信器	
3 0	衛星放送受信アンテナ	
3 1	チューナー/復調器	
3 2	プロセッサ	
3 3	メモリ	
3 4	システムバス	
3 5	スマートカードリーダー	20
3 6	モデム	
3 7	イーサネット(登録商標)カード	
3 8	スマートカード	
3 9	IPパケット	
4 1	IPヘッダ	
4 2	イーサネット(登録商標)フレーム	
4 3	プリアンブル	
4 4	宛先アドレス	
4 5	ソースアドレス	
4 6	タイプ	30
4 7	CRCチェックサム	

---

フロントページの続き

(74)代理人 100107836

弁理士 西 和哉

(74)代理人 100108453

弁理士 村山 靖彦

(74)代理人 100110364

弁理士 実広 信哉

(72)発明者 カーシック・ランジャン

アメリカ合衆国・ノースキャロライナ・28601・ヒコリー・サークル・エヌ・イー・ナインテ  
ィーンズ・アヴェニュー・1992

F ターム(参考) 5C063 AB03 AB05 AC01 AC10 CA23 CA36 DA07 DA13

5C064 BA01 BB05 BC11 BC16 BC20 BD08

5J104 DA04

5K030 GA08 GA15 HA08 HB02 HD01 JA11 JT02 KA19